**中国医学科学院肿瘤医院**

**信息等级保护咨询与集成项目技术需求书**

**2015年6月**

目录

[一、 项目描述 3](#_Toc420676112)

[1.1项目背景 3](#_Toc420676113)

[1.2项目目标 3](#_Toc420676114)

[1.3项目实施要求 3](#_Toc420676115)

[二、招标技术需求 4](#_Toc420676116)

[2.1信息系统的差距分析与整改方案制定 4](#_Toc420676117)

[2.2整改方案的实施 7](#_Toc420676118)

[2.3信息安全培训服务 8](#_Toc420676119)

[2.4第三方测评服务 8](#_Toc420676120)

[三、项目交付清单 9](#_Toc420676121)

[四、项目保密要求 10](#_Toc420676122)

[五、服务方式 11](#_Toc420676123)

[六、资质要求 11](#_Toc420676124)

[七、售后运维服务 12](#_Toc420676125)

**中国医学科学院肿瘤医院**

**信息等级保护咨询与集成项目技术需求书**

## 项目描述

### 1.1项目背景

随着医院信息化的发展，医院信息系统功能越来越趋于完善。医院的日常各项工作已经离不开信息系统的支持。医院信息系统的稳定性和安全性变得尤为关键。

医院信息系统（HIS,以下简称HIS系统）承载着医疗信息、经济信息、病患信息等，一旦泄露对社会秩序构成重大影响；业务中断使医院正常运营蒙受重大经济损失；遭到入侵、篡改等侵害导致业务系统被破坏，会对公民的生命安全和合法权益造成影响和损害。

结合国家相关发文与自身信息系统重要程度，我院决定将HIS系统的安全等级定为三级。

参考《信息安全技术信息系统安全等级保护基本要求》（GB/T22239-2008），从网络、主机等各方面对HIS系统乃至其它系统进行系统的安全整改建设。

### 1.2项目目标

合作方应帮助院方完成HIS系统的三级等级保护测评工作的通过。

项目包含的工作内容有：差距分析、制定整改方案、整改方案实施（不含设备采购）、第三方测评。其中整改方案中应体现我院信息安全长远建设的方向与策略，提供一套可持续建设、不断完善的信息安全体系架构建设方案。

### 1.3项目实施要求

* **不影响现有系统运行**

整个项目周期中应不出现系统中断运行意外事故。

* **设备重复利用**

考虑到未来数据中心建设问题，此次建设中涉及设备应最大程度满足可重复利用原则。即考虑未来设备下线再调整上线的需求，并完成设备下线再调整上线的相应实施工作。

* **通过测评**

合作方应满足“三级等保测评必须通过”的硬性要求。

## 二、招标技术需求

### 2.1信息系统的差距分析与整改方案制定

信息安全咨询服务的主要目标是分析肿瘤医院信息系统的现状，识别并评估其面临的安全风险，提出对应的风险控制措施，形成信息系统安全整改方案。具体工作内容包括：

#### 2.1.1信息系统的差距分析

##### 2.1.1.1信息系统安全现状分析

通过访谈调研、漏洞扫描及渗透测试了解肿瘤医院HIS系统的信息安全现状，针对收集到的信息进行综合分析，并将安全现状与标准中的安全控制措施进行差距分析。

1. 访谈调研的主要内容
* 调研IT组织情况；
* 调研信息系统基础设施基本情况；
* 调研安全管理措施及弱点；
* 调研物理安全控制措施及弱点；
* 调研网络架构安全控制措施及弱点；
* 调研网络设备安全控制措施及弱点；
* 调研操作系统安全控制措施及弱点；
* 调研系统软件安全控制措施及弱点；
* 调研数据库系统安全控制措施及弱点；
* 调研应用系统安全控制措施及弱点。
1. 漏洞扫描

通过手工检查及工具扫描，检查涉及HIS系统安全的各种网络设备、操作系统、系统软件、数据库、应用系统安全控制及弱点情况。

##### 2.1.1.2风险分析及评估

按照《信息安全技术信息系统安全等级保护基本要求》（GB/T22239-2008）、《信息安全技术 信息系统安全等级保护测评要求 》、《信息系统等级保护安全设计技术要求》等国家标准，对现状分析阶段识别的资产中存在的威胁及弱点进行评估，确定资产风险等级，形成风险评估报告。

1. 威胁评价

评估肿瘤医院HIS系统威胁发生的可能性。

1. 弱点评价

评估肿瘤医院HIS系统弱点严重程度。

1. 风险评价

结合肿瘤医院信息系统威胁评价、弱点评价结果，评估HIS系统面临的风险。

##### 2.1.1.3风险处置方案制定

确定HIS系统风险点，选择相应的安全控制措施，制定风险处置方案。避免项目实施过程中与运维过程中出现不可预计的风险事件发生。

1. 确定风险处置方式

确定风险接受准则，并依据准则选择风险处置方式，对于确定为控制的风险，选择具体安全控制措施。

1. 制定风险处置计划

对确定为控制的风险，制定相应的风险处置计划，包括任务、人员、时间安排。

#### 2.1.2信息系统的安全体系整改方案设计

根据HIS系统的差距分析和风险评估结果，规划和建立肿瘤医院信息安全体系，具体工作任务包括：

##### 2.1.2.1管理体系规划设计

针对肿瘤医院信息安全管理现状和需求，规划设计信息安全管理体系，包括：安全管理组织体系、安全管理制度体系，要求形成的组织体系及安全管理制度体系必须满足《信息安全技术信息系统安全等级保护基本要求》（GB/T22239-2008）中的相关管理要求。

1. 安全管理组织体系

形成包含信息安全领导小组、信息安全管理组织、信息安全执行工作组织等安全管理组织。

1. 安全管理制度体系

针对安全活动中的各类管理内容，覆盖物理、网络、主机系统、数据、应用、管理、制度评审、文档控制等各个方面，形成包含信息安全方针、安全策略、安全制度、操作流程等体系化的管理制度。

##### 2.1.2.2技术体系规划设计

依据风险评估结果以及安全标准中的安全控制措施要求，形成肿瘤医院信息安全技术体系建设解决方案（整改方案），要求该解决方案可以满足《信息安全技术信息系统安全等级保护基本要求》（GB/T22239-2008）中的相关技术要求。

应结合医院具体情况，设计《安全设备与系统列表》，并对未来整改工作设计分步实施计划。

### 2.2整改方案的实施

 结合“整改方案”，对方案实施过程中的相关工作，为第三方提供支持。使整套安全体系架构，满足整改方案要求，达到通过三级测评通过要求。内容至少包括以下方面：

1. 物理环境涉及的整改内容；
2. 网络结构整改涉及的配置调整；
3. 新增安全设备涉及的策略部署；
4. 主机、系统、应用层面安全整改所涉及的配置调整；
5. 数据安全整改涉及的结构与策略调整；

### 2.3信息安全培训服务

针对肿瘤医院不同级别的人员，提供针对性的信息安全培训，提升全院人员对信息安全的认识和理解，提升安全管理人员的安防技能及安全管理水平。

### 2.4第三方测评服务

#### 2.4.1总体要求

完成肿瘤医院HIS系统等级保护的第三方测评工作，出具符合信息系统等级测评要求的测评报告。

#### 2.4.2等级保护测评内容

##### 2.4.2.1安全技术测评

完成包括物理安全、网络安全、主机系统安全、应用安全和数据安全等五个方面的安全测评。

##### 2.4.2.2安全管理测评

完成包括安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个方面的安全控制测评。

#### 2.4.3测评结果

在肿瘤医院HIS系统的等级保护定级认证过程中，服务商应配合肿瘤医院完成相关等保定级测评工作，并确保肿瘤医院HIS系统一次性通过等保三级定级测评认证。

## 三、项目交付清单

|  |  |  |
| --- | --- | --- |
| **咨询阶段** | **主要任务** | **文档交付物（纸介质含电子版）** |
| 信息系统的差距分析 | 安全现状分析 | 《信息系统安全现状调研过程文档》《信息系统安全现状分析报告》《差距分析报告》 |
| 风险分析及评估 | 《风险评估报告》 |
| 应急预案制订 | 《风险处置方案》 |
| 信息系统的安全体系整改方案设计 | 管理体系规划 | 《信息系统安全管理制度》 |
| 技术体系规划 | 《信息安全技术体系建设规划报告》《安全设备与系统列表》 |
| 信息安全培训服务 | 信息安全内训 | 所有培训课件 |
| 等级保护定级测评服务 | HIS系统定级测评 | 《HIS系统安全等级三级测评报告》 |

## 四、项目保密要求

要求投标方对项目实施过程中所获得数据及文档等保密信息，承担以下保密义务：

 1、中标方应按要求与（略）签署保密协议。

 2、主动采取保密措施对上述所列信息进行保护，防止不承担同等保密义务的任何第三者知悉及使用。

 3、不得刺探或者以（略）不正当手段（包括利用计算机进行检索、浏览、复制等）获取与本职工作或本身业务无关的甲方关于该项目的商业秘密。

 4、不得向不承担同等保密义务的任何第三人披露甲方关于该项目的商业秘密。

 5、不允许（包括出借、赠与、出租、转让等行为）或协助不承担同等保密义务的任何第三人使用甲方关于该项目的商业秘密。

6、不论何种原因终止参与甲方关于该项目的工作后，都不得利用该项目之商业秘密为（略）企业（包括自办企业）服务。

7、该项目的商业秘密所有权始终全部归属甲方，乙方不得利用自身对项目不同程度的了解申请对于该项目的商业秘密所有权，在本协议签订前乙方已依法具有某些所有权者除外。

8、如发现甲方关于该项目的商业秘密被泄露或者自己过失泄露秘密，应当采取有效措施防止泄密进一步扩大，并及时向甲方报告。

## 五、服务方式

在项目过程中，服务商咨询顾问必须以驻场形式，完成所有服务项目。

从入院开展项目工作开始，时间计划如下：

1. 差距分析相关工作结束，报告文档完成时间为45 天。
2. 整改方案实施，从设备到位至方案实施完成时间为2个月。
3. 测评过程时间为1个月。
4. 整个项目的进度安排应当结合医院新机房建设情况，过程中做适当调整。

## 六、资质要求

1．必须在中华人民共和国注册，具有独立法人资格企业，且要求注册资金不少于人民币500万元；

2．合作方应在[信息](http://info.interscm.com/order/201203/14-553132.html)安全服务方面必须具备成熟案例，且应提供相应的证明文件,如中标通知、合同、验收证书等；

3．合作方必须具有完成本项目的技术力量、财务能力，并且信誉良好。必须具备如下条件：

1. 信息系统集成资质三级（含三级）以上；
2. 具备专业的安全咨询团队，参与安全咨询服务人员至少具备一项 CISSP、CISP、CISA相关安全资质认证,且应提供相应的证明文件；
3. 参与人员不少于5人；
4. 累计在现场不少于150人天；
5. 应提供本地化技术支持能力，具备完善的服务保障体系；
6. 应具备ISO9000质量管理体系认证证书。

4.等级保护测评机构需具有法人资格或其分支机构，能在国内合法提供相应服务的信息安全等级保护测评机构，提供投标企业营业执照副本复印件（加盖公司公章）；

5．等级保护测评机构具有国家或北京市安全等级保护工作协调小组办公室颁发的《信息安全等级保护测评机构推荐证书》，以及公安部信息安全等级保护评估中心颁发的《信息安全等级保护测评机构能力评估合格证书》，提供以上证书复印件（加盖公司公章）。

## 七、售后运维服务

测评结束后，不少于1年的7\*24小时的技术支持服务。技术支持服务包括以下内容：

* 1. 提供24小时热线电话支持、专用技术服务网站支持、Email支持和传真支持等；
	2. 现场技术支持服务：如远程技术支持无法解决的问题，应根据实际工作需要，提供现场支持服务；
	3. 应急响应服务：如发生重大安全事件，应迅速响应用户服务请求，保证在2小时内安排资深安全专家到达现场；
	4. 应提供信息安全等级保护工作的后续整改方案。